NIKSUN® Filters

White Paper
Version 2005

www.niksun.com

NIKSUN, NetVCR, and NetDetector are either registered trademarks or trademarks of NIKSUN, Inc. in the United States and/or other countries.

Ethernet is a trademark of Xerox Corp.
Netscape Communicator is a trademark of Netscape Communications Corporation.
Internet Explorer is a trademark of Microsoft Corporation.
Snort is a trademark of SourceFire, Inc.

NetDetector Snort® IDS and NetVCR Real Time Xperts (NetRTX) are distributed under the terms of GPL (GNU General Public License) and the original code has been modified by NIKSUN. The modified source code can be obtained from http://www.niksun.com/products/snort.html.

Other product and company names mentioned herein may be the trademarks of their respective owners.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

This product includes libpcap and tcpdump software that is copyrighted by the Regents of the University of California. Copyright (c) 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997 The Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that: (1) source code distributions retain the above copyright notice and this paragraph in its entirety, (2) distributions including binary code include the above copyright notice and this paragraph in its entirety in the documentation or other materials provided with the distribution, and (3) all advertising materials mentioning features or use of this software display the following acknowledgement: ``This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors." Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED ``AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Copyright © 2005 NIKSUN, Inc.

This publication is protected by International Copyright Law. No part of this publication may be reproduced, stored in a retrieval system, translated, transcribed, or transmitted in any form, or by any means manual, electric, electronic, electromagnetic, mechanical, chemical, optical, or otherwise, without prior written permission from NIKSUN, Inc. NIKSUN makes no warranty of any kind with respect to this material and disclaims any implied warranty of merchantability or fitness for a particular purpose.

NIKSUN, Inc.
1100 Cornwall Road
Monmouth Junction, NJ 08852
USA
Telephone: (732) 821-5000
Fax: (732) 821-6000
Customer Support: (888) 821-2003
E-mail:info@NIKSUN.com

Table of Contents

Table of Figures ..... **v**

About This Guide ..... **vi**

Objectives vi
Audience vi
Organization vi
Document Conventions vii

Chapter 1: Introduction **8**

What Are Filters? 8
NIKSUN Filters 8
Applications 9
Traffic Recording 9
Virtual Interfaces 9
Traffic Analysis 9
Traffic Alerts 10
Data Replay, NetUsage, and Filtered Archive 10
Reports 10
Packet Dump 10

Chapter 2: Filter Expressions **11**

Overview 11
Filter Syntax 11
Protocol Qualifiers 11
Direction Qualifiers 13
Type Qualifiers 13
Summary of Qualifiers 15
Examples of Basic Filter Expressions 15
Combining Filter Expressions 18
Examples of Combined Filter Expressions 18
Complex Filter Expressions 19
Examples of Complex Filter Expressions 20
Variable Length Filtering (VLF) 21
Examples of Variable Length Filtering 21
Combining the ”not” Operator with Variable Length Filtering 22
Filtering Broadcast and Multicast Traffic 23
Filtering Outbound and Inbound Traffic 23
Filtering ICMP Traffic 23
Filtering IP Traffic Using TOS and DiffServ 24
Filtering Fragmented IP Traffic 24
The Filter Expressions 24
Filtering Unrecognized Traffic 25
The Filter Expressions 25

Chapter 3: Using Filters **26**

Using Filters in NetDetector/NetVCR 2005 26
Recording Configuration 27
Dataset Configuration 27
Virtual Interfaces 28
Filtered Archive 29
Alarm Configuration 29
Traffic Analysis 31

Analysis Start Screen....31
Traffic Analysis: Main Screen....32
Host Pairs....32
View Packets....34
TCP Connections Tables....35
TCP Analysis Tables....35
TCP Performance Tables....36
WWW Abort Tables....36
Archive Packet Data....37
Replay Data....37
Application Reconstruction....37
Data Management....38
On-demand Export....38
NetUsage....39
NetReporter for NetDetector....40
NetReporter for NetVCR....40
Using Filters in NetVoice....41

Frequently Asked Questions....44

Table of Figures

Figure 1-1: Traffic analysis statistics are retrieved and displayed to the user 10
Figure 2-1: Summary of qualifiers that are used in filter expressions 15
Figure 2-2: IP packet header 17
Figure 2-3: UDP packet header 17
Figure 2-4: TCP packet header 17
Figure 2-5: Ethernet frame 18
Table 3-1: Features in Appliance that accept filter expressions that are input by the user 26
Figure 3-1: The Dataset Configuration screen S P R 28
Figure 3-2: Create Virtual Interface screen S P R 28
Figure 3-3: The Filtered Archive screen S P 29
Figure 3-4: The Alarm Configuration screen S 31
Figure 3-5: The Start screen S 31
Figure 3-6: The Analysis screen S 32
Figure 3-7: Host Pairs Tables screen S 34
Figure 3-8: The View Packets screen S P 34
Figure 3-9: The TCP Connections screen S 35
Figure 3-10: TCP Analysis tables S 35
Figure 3-11: TCP Performance Tables screen S 36
Figure 3-12: WWW Abort Tables screen S 36
Figure 3-13: The Archive Packet Data screen S P 37
Figure 3-14: The Replay Data screen S P 37
Figure 3-15: Application Reconstruction screen S 38
Figure 3-16: Reconstructed web page 38
Figure 3-17: On-demand Export screen S P 39
Figure 3-18: The NetUsage Configure Capture Qualifiers screen S 39
Figure 3-19: The NetReporter screen S 40
Figure 3-20: The NetReporter screen S 40
Figure 3-21: The NetVoice Main Screen S 41
Figure 3-22: Call View Screen S 42

About This Guide

This chapter explains the objectives, audience, organization, and conventions that are used in this document.

Objectives

This document aims to explain filters, construction of filter expressions, and their application in NIKSUN products (NetDetector/NetVCR 2005)

Audience

The intended audience is for those who use products developed by NIKSUN, or are interested in the application of network traffic filters.

The document assumes that readers have a working knowledge of the TCP/IP Protocol and its implementation in a network.

Some familiarity with concepts related to network security and intrusion detection and analysis would also be beneficial.

Organization

This document is arranged into the following chapters:

- **Chapter 1: Introduction**
  This chapter introduces filters and describes the application of NIKSUN filters.

- **Chapter 2: Filter Expressions**
  This chapter explains the filter syntax and how to construct filter expressions. Examples are provided.

- **Chapter 3: Using Filters**
  This chapter explains how filters are used by various features in NIKSUN appliances.

- **Frequently Asked Questions**
  This chapter answers frequently asked questions.

Document Conventions

The text-style conventions are described in the table below.

Convention	Description
Boldface	New terms, screen titles, and screen elements the first time they are mentioned.
`On-screen Command`	Commands to be entered by the user.
`On-screen Text`	Computer output.
< >	Encloses any text that is non-printed, but must be replaced with relevant information.
Hyperlinks	Click on the hyperlinks to go to the section of the document where the hyperlinked terms are explained in detail.

Chapter 1: Introduction

What Are Filters?

Filters are software that examine and qualify network traffic data. Based on the criteria specified by filters, data is either rejected or qualified for use by the application that has applied filters. The applications are explained in the following sections.

NIKSUN Filters

NIKSUN's traffic filters are flexible and easy to use. Users can build their own filters or use pre-defined filters to achieve a variety of results. Filter expressions can be applied at any protocol layer.

NIKSUN filter syntax is based on the BPF syntax (Berkeley Packet Filter), used by UNIX utilities such as *libpcap*, *tcpdump*, and *snoop.*

Data can be broadly classified into two types:

- **Raw packets**
  Network traffic that is captured and recorded by the NIKSUN equipment.

- **Statistics**
  Statistics of the raw packets that is generated and stored by NIKSUN's statistical processing engine. (**Note**: Based on the protocol layer, different types of statistics are generated.)

Both types of data are stored in the database. Filters can be applied to both.

Filters are generally applied to stored data, except during traffic recording when they are applied to incoming traffic data. Filters can be broadly classified into three types:

- **Statistics filters**
  Statistics filters, applicable at the level of stored statistical records, are used by applications that read traffic statistics from the database.

- **Packet filters**
  Packet filters, applicable at the level of individual data packets, are used by applications that read raw-packet data from the database.

- **Recording filters**
  Recording filters, applicable at the level of individual data packets, are used by applications that record network traffic. Complex recording filters can significantly lower the performance of the recording application.

The three types of filters are related in the following way:

- Statistics filters can also be used as packet filters.

- Statistics filters and packet filters can also be used as recording filters.

Important: The icons for each of the filter types (described above) are used to classify all the examples of filter expressions. The specific product features/screens are also classified by these icons. This information would help in applying appropriate filter expressions to each feature.

Applications

NIKSUN products use filters in various applications, which are summarized in this section. The applications are explained in detail in Chapter 3:.

The applications are:

- **Traffic Recording** S P R
- **Virtual Interfaces** S P
- **Traffic Analysis** S
- **Traffic Alerts** S
- **TCP Replay, File Export,** and **Selective Archive** S P
- **Reports** S
- **Packet Dump** S P

Traffic Recording

In this application, recording filters are applied to network traffic while it is being recorded. This results in better usage of storage media and system resources. For example, traffic that does not represent a security threat or specific interests (i.e. from a known host) can be filtered out.

Advanced filtering options include Variable Length Filtering, where a specified number of bytes are kept from each packet (see the section on Variable Length Filtering (VLF)).

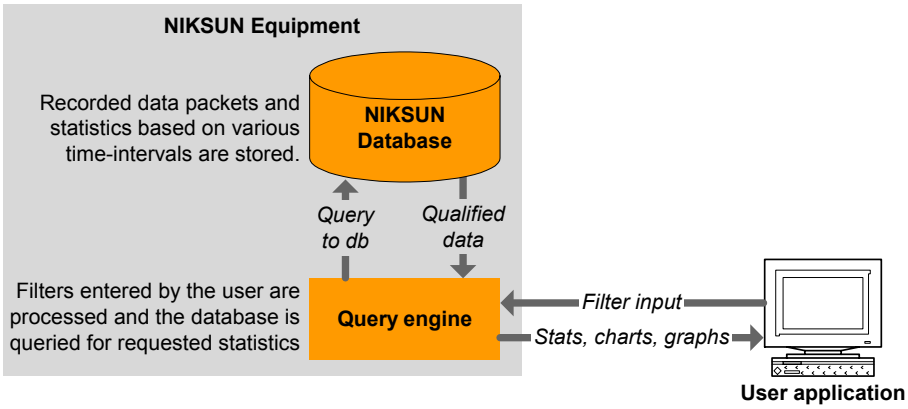
Virtual Interfaces

Virtual interfaces can represent a combination of two or more physical interfaces, or a subset of traffic on a physical interface. In this application, filters are applied to traffic on a virtual interface.

Traffic Analysis

In this application, filters are applied to stored traffic statistics. For example, specific information such as traffic originating from a particular host or subnet can be filtered and displayed to the user as plots and tables. Figure 1-1 explains how statistics are retrieved and displayed to the user.

Figure 1-1: Traffic analysis statistics are retrieved and displayed to the user


NIKSUN Equipment
Recorded data packets and statistics based on various time-intervals are stored.
NIKSUN Database
Query to db
Qualified data
Filters entered by the user are processed and the database is queried for requested statistics
Query engine
Filter input
Stats, charts, graphs
User application

Traffic Alerts

Traffic alerts notify users when the network traffic crosses pre-defined thresholds. Traffic Alerts use filters to detect these occurrences. For example, users can be notified if the bandwidth used by an application or a subnet crosses a pre-defined threshold.

Data Replay, NetUsage, and Filtered Archive

Filters are used by these applications to filter specific packets for replay, export, or archive operations. For example, all port-80 traffic on the network can be selectively archived.

Reports

Reports are generated on-demand or scheduled on recorded datasets. Based on user inputs, filters qualify the results that are to be reported. For example, users can choose to generate reports (containing statistics, graphs, and charts) on the busiest hosts on the network.

Packet Dump

Filters qualify the packets that are to be exported (generated) by the packet dump application.

Chapter 2: Filter Expressions

Overview

The applications, described in the previous sections, require the user to enter filter expressions. This section explains what filter expressions are, and how they are constructed.

Filters can be network layer-specific; care must be taken to ensure that they are applied at the appropriate layer; otherwise, no data would be displayed.

Filter Syntax

It is important to be aware that although all filter expressions follow the same syntax, they are specific to the data types (i.e. raw packets or statistics) and protocol layers. To obtain valid results, data types and protocol layers have to be carefully considered.

Filter expressions, in the BPF syntax, consist of one or more primitives. Each primitive consists of one or more qualifiers, followed by a value, which can be an identifier or a number.

```
<qualifier> <value>
```

Qualifiers fall into three categories:

- Protocol
- Direction
- Type

Qualifiers from each category can be combined together as shown by the following general form:

<protocol qualifier> <direction qualifier> <type qualifier> <value>

Each qualifier category is optional, but at least one of the three categories of qualifiers must be referenced in a filter primitive.

The following sections explain each of the qualifier categories and the various combinations in detail.

Note: All filter expressions must be in lowercase letters.

Protocol Qualifiers

Protocol qualifiers are used to filter for a particular protocol. They can be used with or without a value.

Valid protocol qualifiers include:

- **ether**
  Ethernet

- **fddi**
  Fiber Distributed Data Interface

- **ip**
  Internet Protocol

- **arp**
  Address Resolution Protocol

- **rarp**
  Reverse ARP

- **tcp**
  Transmission Control Protocol

- **udp**
  User Datagram Protocol

- **ppp**
  Point-to-Point Protocol

Note: If a protocol is not specified, **ip** is the assumed default.

Examples of filter expressions that use protocol qualifiers:

- **ether host 02:07:01:00:01:c4**
  Filters all Ethernet traffic originating from or destined for 02:07:01:00:01:c4 (hex).

  Note: If this expression is used as a " filter", it is valid only for Ethernet interfaces that have been configured for VLAN, because only VLAN statistics contain MAC addresses. This expression, when used as a statistics filter on non-VLAN interfaces, would not return a result.

- **tcp src port 21**
  Filters all TCP traffic that originates from port 21.

Abbreviations

Abbreviations for **ether proto <p>** where **<p>** is one of the following protocols:

- **ip**

- **arp**

- **rarp**

- **decnet**

Important: Back-slash "\" is used to distinguish names from being interpreted as reserved words in the syntax. For example, **ether proto \ip** (see above) or **ip proto \tcp** (see below).

Abbreviations for **ip proto <p>** where **<p>** is one of the following protocols:

- **tcp**
- **udp**
- **icmp**

Direction Qualifiers

Direction qualifiers are used to specify a transfer direction with regard to the ID. Valid direction qualifiers are:

- **src**
  Specifies a transmission source.
- **dst**
  Specifies a destination.
- **src and dst**
  Specifies both, a transmission source and a destination.
- **src or dst**
  Specifies either a transmission source or a destination.

Note: If a direction qualifier is not specified, **src or dst** is the assumed default.

Examples of filter expressions that use direction qualifiers:

- **src 12.34.3.1**
  Filters all traffic originating from the specified host name where 12.34.3.1 is the host IP address.
- **dst net 123.156**
  Filters all traffic destined for the network 123.156.
- **src and dst port 20**
  Filters all traffic originating from and destined for port 20.

Type Qualifiers

Type qualifiers specify the identifier. This is used to denote the target for the search. Type qualifiers include:

- **host** <host name or IP address or MAC address>
  Refers to a host on the networks that are being monitored.
- **net** <IP address>
  Refers to a network (or a subnet on a network).

- **port** <number or port name>
  Refers to a port.

- **proto** <protocol name or number>
  Refers to a protocol. This qualifier is applicable on the data link layer when the protocol qualifier (described later in this document) is **ether**, **fddi**, or **ppp**. It is also applicable on the network layer when the protocol qualifier is **ip.**

- **tlink** <number>
  Refers to a link on a serial interface (T1/E1, T3/E3).

- **tchannel** <number>
  Refers to a channel on a serial interface (T1/E1, T3/E3).

- **dlci** <number>
  Refers to a Data Link Connection Identifier for a logical circuit on a frame relay network.

- **vpi** <number>
  Refers to a Virtual Path Identifier on an ATM network.

- **vci** <number>
  Refers to a Virtual Circuit Identifier on an ATM network.

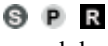
- **vlan** <number>
  Refers to a Virtual LAN identifier.

- **ftype** <number>
  Refers to the frame type. **ftype** is used to uniquely identify each type of link layer protocol running on a link.

- **mask** <ID in dotted decimal form or "/" followed by subnet mask length in bits>
  Refers to a subnet mask. This is used with the **net** type. The ID can be specified in the dotted-decimal form, or by the length (in bits) of the subnet mask, preceded by a slash.

Examples of filter expressions that use type qualifiers:

- **host anyhost.niksun.com**
  Filters all traffic originating from, and destined for anyhost.niksun.com

- **host 123.156.189.12** 
  Filters all traffic originating from, and destined for 123.156.189.12

- **port 20**
  Filters all port 20 traffic.

- **port ftp**
  Filters all ftp-port traffic.

- `net 123.156`
- `net 123.156 mask 255.255.0.0`
- `net 123.156/16`

  The three expressions, listed above, filter all traffic on the network 123.156.

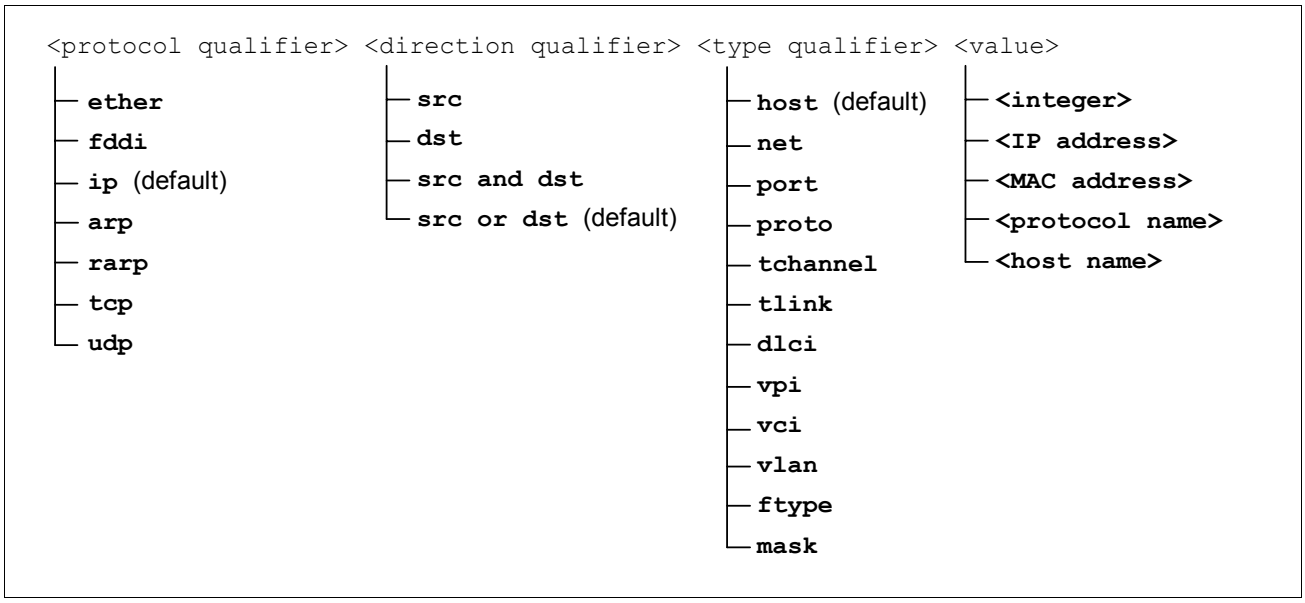
- `proto 17`

  Filters all UDP traffic.

Summary of Qualifiers

Figure 2-1 summarizes the qualifiers that have been described above.

Figure 2-1: Summary of qualifiers that are used in filter expressions



Examples of Basic Filter Expressions

The following examples illustrate the use of qualifiers that are described in the previous section:

- `dst host 10.0.0.5`

  Filters all traffic destined for the host address 10.0.0.5.

- `src host www.yahoo.com`

  Filters all traffic originating from the host www.yahoo.com.

- `host 10.20.3.4`

  Filters all traffic originating from or destined for the host address 10.20.3.4.

- **`ether src host 02:07:01:00:01:c4`** S P R
  Filters all Ethernet traffic originating from 02:07:01:00:01:c4 (hex). Refer to the note in the previous example.

- **`dst net 10.0`** S P R
  Filters all Ethernet traffic destined for the network 10.0.

- **`src net 10.0.0/24`** S P R
  Filters all traffic originating from the network 10.0.0 with the 24-bit mask (after the forward-slash).

- **`src and dst net 10.0.0 mask 255.255.224.0`** S P R
  Filters all traffic originating from and destined for the network 10.0.0 with the mask 255.255.224.0.

- **`tcp port http`** S P R
  Filters all Ethernet traffic originating from or destined for the HTTP port.

- **`port domain`** S P R
  Filters all UDP or TCP traffic (used by DNS services).

- **`ip proto ospf`** S P R
  Filters all IP traffic using the IP protocol 89, which is assigned to the OSPF (Open Shortest Path First) routing protocol. See `/etc/protocols` for the names of assigned IP protocols.

- **`ip proto \tcp`** S P R
  Filters all IP traffic that uses the TCP protocol.

  Note: Since **`tcp`** can also be used as a keyword, in this example it is preceded by a backslash "\". Other terms that need to be similarly differentiated are **`udp`** and **`icmp`**.

- **`vlan 1`** S P R
  Filters all traffic that has a vlan identifier of 1.

- **`ftype 33024`** S P R
  Filters all traffic that has the frame type 33024. In this case, **`ftype 33024`** corresponds to the VLAN protocol `802.1q`.

- **`ether proto \ip`** S P R
  Filters all IP traffic on the Ethernet protocol.

- **`dlci 13`** S P R
  Filters all traffic that has a DLCI identifier of 13 on the frame-relay network.

- **`tlink 1`** S P R
  Filters all traffic on the serial interface that has a link identifier of 1.

Note: The protocol layer has to be considered while applying the filters. For example, a **host** filter will not work at the data link level because the data link level traffic does not recognize IP addresses or host names.

For description on packet headers for various protocols, refer to Figure 2-2, Figure 2-3, Figure 2-4, and Figure 2-5. Only the fields that are shaded in gray are accessible by statistics filters while packet filters can access all the bits. In Figure 2-5, MAC addresses are stored as statistics only for traffic on Ethernet interfaces that have been configured for VLAN.

Figure 2-2: IP packet header

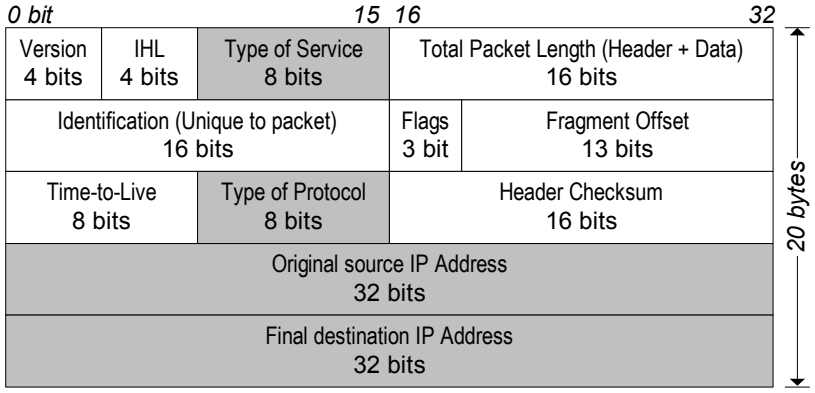


Figure 2-3: UDP packet header

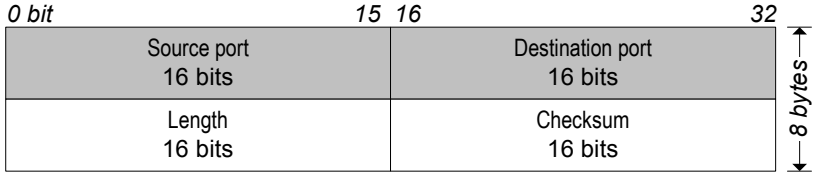


Figure 2-4: TCP packet header

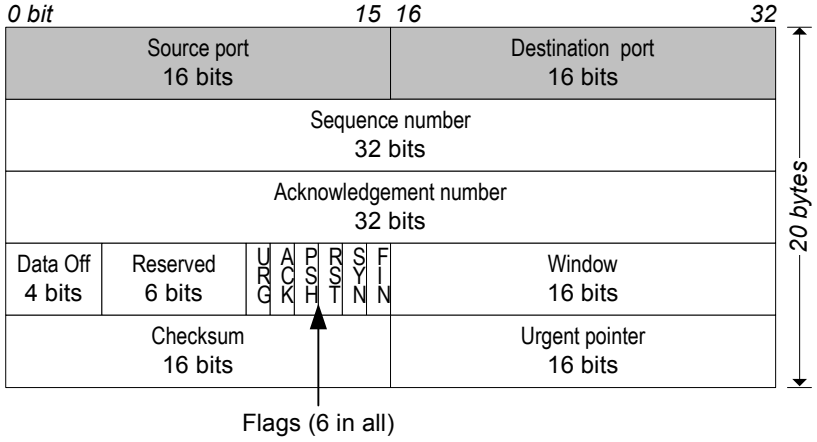
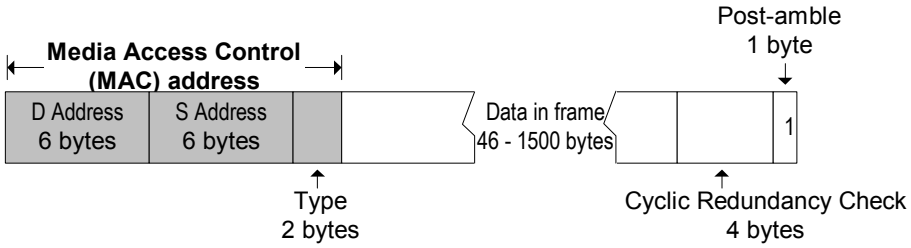


Figure 2-5: Ethernet frame



Combining Filter Expressions

Filter expressions can be combined by using the logical operators:

- Negation (**!** or **not**)
- Concatenation (**&&** or **and**)
- Alternation (**||** or **or**)

Examples of Combined Filter Expressions

Examples of combined filter expressions are listed below:

- **src 123.156.189.10 or src 123.156.189.12** S P R
  The first part of the expression, **src 123.156.189.10**, filters traffic originating from **123.156.189.10**

  The second part, **src 123.156.189.12** filters traffic originating from **123.156.189.12**

  The combined expression filters traffic originating from either of the two hosts.

- **host 20.3.2.1 and port 80** S P R
  The first part of the expression, **host 20.3.2.1**, filters all traffic originating and destined for the host **host 20.3.2.1**.

  The second part, **port 80**, filters traffic originating from or destined for the specified port number. The combined expression filters all port-80 traffic that has **host 20.3.2.1** as a source or a destination.

- **not ip net 123.156** S P R
  All IP traffic on the subnet 123.156 is excluded by using the **not**. As a result, traffic other that the one going to or from the 123.156 subnet is qualified

- **not (host 2.3.1.3 and host 2.3.1.4)** S P R
  Can also be written as **not host 2.3.1.3 or not host 2.3.1.4**

  Parentheses can be used with logical operators. This filter excludes all traffic between the two hosts.

- **tcp dst port ftp ‖ tcp dst port ftp-data ‖ tcp dst port domain**
  Can also be written as **tcp dst port ftp ‖ ftp-data ‖ domain** S P R

  To contract the expression, identical qualifier lists can be omitted. This filter qualifies all TCP traffic destined for the ftp, ftp-data, or domain ports.

- **not dst host 2.3.1.3 && host 2.3.1.4** S P R
  Will be understood as **not dst host 2.3.1.3 && dst host 2.3.1.4**

  If an identifier is entered without a qualifier, the most recent qualifier is assumed. This filter qualifies all traffic that is not destined for **host 2.3.1.3** and is destined for **host 2.3.1.4**.

- **(udp port 161 or 162) and not src net 172.17** S P R
  The first part of the expression, **(udp port 161 or 162)**, filters for SNMP traffic on ports 161 or 162.

  The second part of the expression **not src net 172.17** excludes all traffic on the 172.17 subnet.

  The complete expression when combined by **and**, filters UDP traffic on ports 161 or 162 that is not on the subnet 172.17.

Complex Filter Expressions

A larger selection of operators and commands can be used to create more complex filter expressions.

The NIKSUN filter syntax supports expressions in the following form:

```
<expr> <relop> <expr>
```

<relop> can be one of the following relational operators: **>**, **<**, **>=**, **<=**, **=**, or **!=**

<expr> is an arithmetic expression composed of any of the following:

- Integer constants (expressed in the standard C syntax)
- Normal binary operators [**+**, **-**, *****, **/**, **&**, **|**]
- **len** Length operator
- Special packet data accessors (to access data inside a packet)

To access data inside the packet, the following syntax is used:

```
<proto> [ <expr> : <size> ]
```
P R

Where **<proto>** can be: **ether, fddi, ip, arp, rarp, tcp, udp, icmp,** or **osfp**. The value indicates the protocol layer for the index operation.

The byte offset, relative to the indicated protocol layer, is specified by <expr>.

<size> is optional and indicates the number of bytes to be read in the field of interest. It can have values of one (default), two, or four.

Examples of Complex Filter Expressions

Examples of complex filter expressions are listed below:

- **`tcp[13:1] & 3 != 0`** P R
  This expression examines the TCP packet header. The first part of the expression, **`tcp[13:1]`**, locates the position after 13 bytes from the beginning of the header and reads 1 byte after that position, i.e., the 14th byte.

  `& 3` performs a bit-wise and operation on the selected byte. A true result would indicate that the SYN or FIN flags are on.

- **`tcp and (tcp[13] & 2 != 0) and (dst port 143)`** P R
  Filters for IMAP SYN packets. The first part of the expression, **`tcp`**, filters for TCP packets. **`tcp[13]`** is also written as **`tcp[13:1]`** (Refer to the previous example). The last part of the example, **`(dst port 143)`**, filters all port-143 traffic.

- **`ip[2:2] > 576`** P R
  Filters all IP packets that are longer than 576 bytes. **`ip[2:2]`** reads two bytes in the IP packet, starting at the third byte of the header. The two bytes form a 16-bit number specifying the packet length.

- **`icmp and icmp[0] != 8 and icmp[0] !=0`** P R
  Filters all ICMP packets that are not echo request and echo reply packets. **`icmp[0]`** reads the first byte of the ICMP header.

- **`ip[0] & 0xf != 5`** P R
  Filters all IP packets with options. The first part of the expression, **`ip[0]`**, reads the first byte of the IP header.

- **`ip[6:2] & 0x2000 != 0`** P R
  Filters all fragmented IP data packets. **`ip[6:2]`** reads two bytes in the IP packet starting at the seventh byte of the header.

- **`ip[6:2] & 0x1fff = 0`** P R
  Filters only un-fragmented data packets and flag zero of fragmented data packets. This check is implicitly applied to the TCP and UDP index operations. For instance, **`tcp[0]`** always refers to the first byte of a TCP header, and never means an intervening fragment.

- **`ip[6:2] &0x1fff < 5 and ip[6:2] &0x1fff  !=0`** P R
  Filters all IP data packets with an offset value less than five but greater than zero, as indicated in the offset field.

- **`ip and ip[12:4] = ip[16:4]`** P R
  Detects data packets that cause a LAND attack. The expression checks if the IP host and destination addresses are the same. Loop back Denial-of-Service (LAND) attack occurs when the source host/port and the destination host/port of the packet are the same. As a result, the packet loops back to the same host, resulting in traffic overload and degraded host/network performance.

- **`ip and ip[19] = 0xff`** P R

- **`ip and net 0.0.0.255 mask 0.0.0.255`**
  The two expressions achieve the same result. Filters IP data packets designated for broadcast.

  The first expression, **`ip and ip[19] = 0xff`**, checks if the twentieth byte in the IP header equals the number specified in hex. If it is equal, it indicates that it is a broadcast packet.

  The second expression **`ip and net 0.0.0.255 mask 0.0.0.255`** also checks if the packet is for broadcast.

Variable Length Filtering (VLF)

Variable length filtering of data packet provides, on a per-packet basis, extensive control over the exact amount of packet data to be captured and permanently stored.

This feature enhances the overall performance of NIKSUN products through optimized control over the total amount of network data to be stored, processed, and managed.

The NIKSUN filter syntax allows the user to specify the amount of bytes per packet to be recorded. For example:

`<F> keep <B>` R

`<F>` is a filtering expression that qualifies the data packets that are to be kept.

`<B>` describes the number of bytes to be kept and can be one of the following:

- A positive integer that specifies the number of bytes to be recorded.

- **`layer L`**
  Where **L** is **2** for data link layer and **3** for network layer (**Note:** Currently, Layer 3 works only for IP packets).

- **`layer L + x`**
  Where **L** is **2** for data link layer and **3** for network layer plus **x** bytes.

- **`all`**
  To record the complete packet.

The **`default keep <B>`** filter term accepts all packets by default.

Examples of Variable Length Filtering

Examples of filter expressions with variable length filtering are listed below:

- **`ether proto 0x8100 keep 32`** R
  32 bytes of the header for all Ethernet protocol data packets are kept.

- **`ether proto 0x8100 keep all`** R
  The complete Ethernet protocol data packet is kept.

- **`ip keep layer 3`** R
  All IP data packets headers from the network layer are kept.

- **`tcp keep layer 3 + 20`** R
  All TCP data packet headers from the network layer along with the first twenty bytes of the TCP header are kept.

- **`ip keep all or default keep 200`** R
  If it is an IP data packet the entire packet is kept, otherwise the first 200 bytes of the packet is kept. (If the packet size is less than 200 bytes, the entire packet is kept.)

- **`tcp keep layer 3 + 20 or udp keep layer 3 + 8 or ip keep layer 3 or default keep layer 2`** R
  The example is explained in parts.

  The first part: **`(tcp keep layer 3 + 20)`** If it is a TCP packet, IP layer headers and an additional 20 bytes are kept.

  The second part: **`(udp keep layer 3 + 8)`** Or, if it is a UDP packet, the IP layer header and an additional 8 bytes are kept.

  The third part: **`(ip keep layer 3)`** Or, if it is an IP packet, the IP layer header are kept.

  The fourth part: **`(default keep layer 2)`** If it is not an IP packet, the data link layer header is kept .

- **`(tcp port http or https keep 200) or (tcp port smtp or pop3 or imap keep all) or default keep 150`** R
  The example is explained in parts.

  The first part: **`(tcp port http or https keep 200)`** If it is TCP traffic on the HTTP or HTTPS ports, then 200 bytes of each packet are kept.

  The second part: **`(tcp port smtp or pop3 or imap keep all)`** Or, if it is TCP traffic on the SMPT, POP3, or IMAP ports, then the entire packet is kept.

  The third part: **`(default keep 150)`** For all other packets, 150 bytes are kept.

Combining the ”not” Operator with Variable Length Filtering

Use the following syntax when using the “not” operator with VLF:

`(not <F>) keep <B>` R

Where **`<F>`** is replaced by the filter expression and **`<B>`** is replaced by the actual number.

Note that parentheses must be used as described above.

Filtering Broadcast and Multicast Traffic

The following qualifiers can be used to filter broadcast and multicast traffic:

- `<protocol qualifier>` **`broadcast`** S P R
  Used after a protocol qualifier. Filters for broadcast packets.

- `<protocol qualifier>` **`multicast`** S P R
  Used after a protocol qualifier. Filters for multicast packets.

Examples of filter expressions that use the keywords:

- **`ip broadcast`** S P R
  Filters all IP broadcast traffic.

- **`ether multicast`** S P R
  Filters all Ethernet multicast traffic.

Filtering Outbound and Inbound Traffic

All outbound traffic on a link can be filtered by the following command, which can be used without any parameters or qualifiers:

`outbound` S P R

The alias for `outbound` is **`egress`**.

Similarly, all inbound traffic on a link can be filtered by the following command, which can be used without any parameters or qualifiers:

`inbound` S P R

The alias for `inbound` is **`ingress`**.

The expressions can be combined with logical operators to create more complex filter expressions. For example, the following expression filters all inbound TCP traffic for the specified host:

`inbound and tcp and host 234.43.21.53` S P R

Note: The system has no way of knowing which portion of the traffic is inbound and which portion is outbound with regard to the user's perspective. Inbound/outbound are relative attributes that are used to distinguish two directions of traffic on a full duplex link.

Filtering ICMP Traffic

To filter ICMP packets based on a **Type** value (RFC 792), use the following syntax:

`itype <n>` S P R

<n> is a number between 0-255.

Similarly, to filter ICMP packets based on a **Code** value (RFC 792), use the following syntax:

```
icode <n>
```

<n> is a number between 0-255.

Filtering IP Traffic Using TOS and DiffServ

To filter IP packets based on a **Type of Service** (ToS) value (RFC 795), use the following syntax:

```
tos <n>
```

<n> is a number between 0-255.

To filter IP packets based on a **DiffServ** (Differentiated Service) value, use the following syntax:

```
diffserv <n>
```

<n> is a number between 0-63.

Filtering Fragmented IP Traffic

IP fragmentation occurs when an IP packet arrives at a gateway and needs to be transported further across a link that has a capacity smaller than the packet size. In this situation, the gateway will either discard the packet if the *Don't Fragment* (DF) bit is set. Otherwise, the packet is divided into a number of smaller packets (i.e., fragments) that can be transported across the link. The fragments are then reassembled at the destination. Fragmentation can occur several times on the way to the destination. When fragmentation occurs, the IP headers from the original packet are copied into each fragment with the following modifications:

- The More Fragments (MF) bit is set for every fragment except the last one.
- The identification number is set to a value unique for the life duration of the packet.
- The length field indicates the length of the fragment, not the original packet.
- The offset field in each fragment is used during reassembly. Together with the length field it indicates which portion of the original packet is contained in the current fragment.

IP fragments are accounted for as a separate class of traffic by NIKSUN software. This traffic can be qualified by filters.

The Filter Expressions

IP traffic can be filtered by using the following keyword:

```
ipfrag
```

The syntax is as follows:

```
ether proto ipfrag
```

The following expression is also valid:

```
ether proto 1498
```

The keyword **type** can be used as an alias for **ether proto**:

```
type ipfrag
```

```
type 1498
```

Filtering Unrecognized Traffic

NIKSUN software accounts for unrecognized frames. An unrecognized frame has one or more of the following properties:

- The frame length is too short or too long to be valid.
- The `ethertype` is invalid.
- The `ethertype` is explicitly set to unknown/reserved by the sender.
- The link layer header(s) is invalid or cannot be decoded.
- The IP header is invalid or cannot be decoded.

Unrecognized frames can be qualified by filters.

The Filter Expressions

Unrecognized traffic can be filtered by using the following keyword (alias):

```
unknown
```

The syntax is as follows:

```
ether proto unknown
```

The keyword **type** can be used as an alias for **ether proto**:

```
type unknown
```

Chapter 3: Using Filters

The chapter describes the use of filters in NIKSUN products - NetDetector/NetVCR 2005, and NetVoice.

Using Filters in NetDetector/NetVCR 2005

In NIKSUN NetDetector/NetVCR 2005, filter expressions are applied to network traffic during recording and to stored statistics and packets during analysis and processing. Table 3-1 describes the screens where filters can be applied.

Table 3-1: Features in Appliance that accept filter expressions that are input by the user

Screen (feature) name[1]	Description	Applicable Filter-type(s)[2]
Recording Configuration		
Dataset Configuration	Configure traffic capture and recording parameters.	
Virtual Interfaces	Define a virtual interface as a qualified subset of traffic from a physical interface.	
Filtered Archive	Define a filter on the basis of which a dataset is filtered and archived.	
Alarm Configuration	Triggers alerts if pre-defined thresholds are crossed.	
Traffic Analysis		
Analysis Start Screen	Quick, high level traffic analysis on stored datasets.	S
Traffic Analysis: Main Screen	Detailed analysis on stored datasets.	S
Host Pairs	Bytes and packets that are transferred between hosts.	
View Packets	Viewing and exporting (PCAP) qualified data.	
TCP Connections Tables	Connections, bytes, packets transmitted and received, for an individual host.	
TCP Analysis Tables	Connections, bytes, packets transmitted and received, for an individual host.	
TCP Performance Tables	Data transmission rates for individual hosts.	
WWW Abort Tables	Displays aborted HTTP connections for servers and clients.	

[1] Refer to the NetDetector/*NetVCR User's Guide* for additional details on the screens.
[2] Refer to **Error! Reference source not found.** for an explanation of filter-types and icons.

Archive Packet Data	Permanently archive a subset of an existing dataset.	
Replay Data	Replay traffic data over any other non-management Ethernet interface.	
Application Reconstruction	Reconstructing TCP applications to investigate unusual traffic.	
Data Management		
On-demand Export	Importing/exporting qualified data via HTTP.	
NetUsage	Exporting Internet Protocol Detailed Records (IPDRs)- used for IP billing.	
Reporting		
NetReporter for NetDetector	Viewing statistical reports in graphical and tabular formats for NetDetector.	
NetReporter for NetVCR	Viewing statistical reports in graphical and tabular formats for NetVCR.	

Recording Configuration

An important application of filters is during recording configuration, as described below.

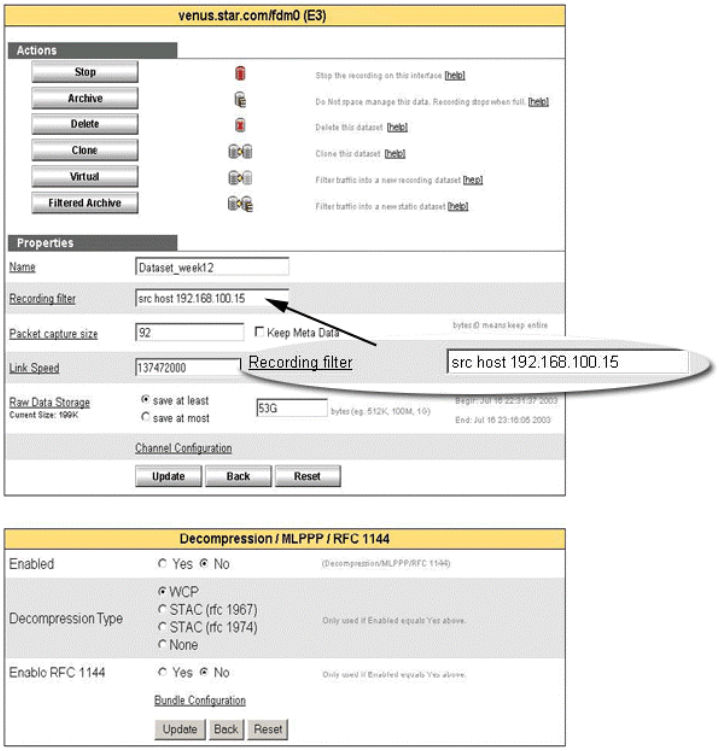
Dataset Configuration

Applicable filter-type(s): S P R

On the **Dataset Configuration** screen (Figure 3-1), traffic-recording parameters are set. Recording filters are used to qualify the traffic that is to be recorded.

Enter the filter expression in the **Recording Filter** text box. After other required parameters have been entered, click the **Update** button to apply the filter.

Figure 3-1: The Dataset Configuration screen S P R



Virtual Interfaces

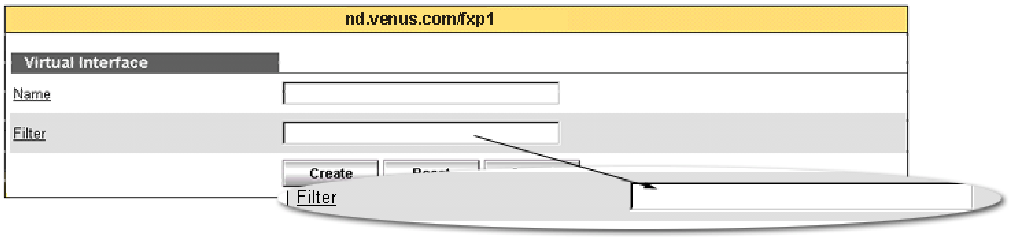
Applicable filter-type(s): S P R

A virtual interface can be defined to represent a subset of traffic from the physical interface. It is important to note that recording filters are used while defining the virtual interface

After the virtual interface has been created, separate statistics are generated for each virtual interface. The various features and screens see the virtual interface as any other interface. When the virtual interface is accessed from all the other screens/features, the same filtering rules apply.

On the Create Virtual Interface screen Figure 3-2, to specify a filter that will be used to create a virtual interface, type the filter in the Qualification text box.

Figure 3-2: Create Virtual Interface screen S P R

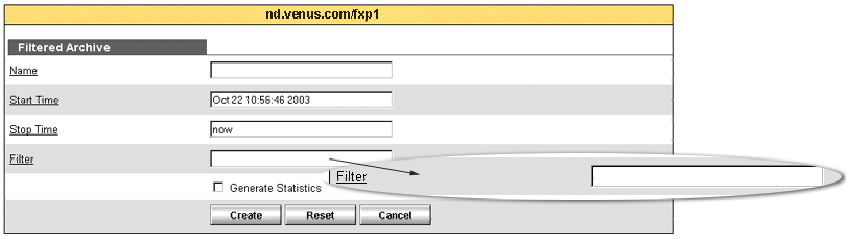


Filtered Archive

Applicable filter-type(s): S P

The **Filtered Archive** option can be selected for the specified dataset on the Dataset Configuration screen. This option enables you to select (using a filter expression and start/stop times) and permanently archive a portion of a dataset. Figure 3-3 shows the Filtered Archive screen.

Figure 3-3: The Filtered Archive screen S P



Alarm Configuration

Applicable filter-type(s): S

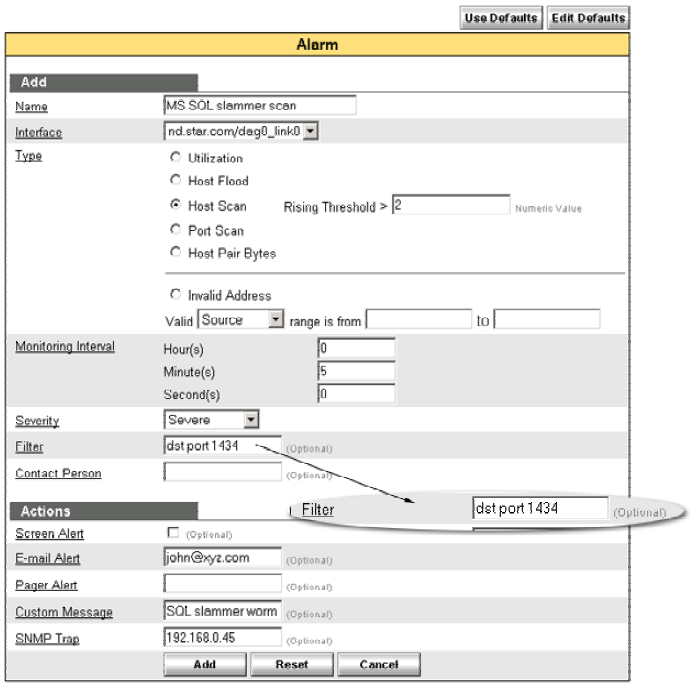
Traffic Alarms notify designated persons if the network traffic crosses pre-defined thresholds. Alarms use filters to detect these occurrences. Alarms that are set by the user include:

- Bandwidth utilization (alert if traffic load crosses preset thresholds)
- Host flooding (alert if multiple host pairs having a common destination exceed limits)
- Host scans monitoring (alert if multiple host pairs having a common source exceed limits)
- Host pair bytes (alert if number of bytes exchanged between host pairs exceeds limits)
- Invalid addresses (alert if a valid IP range, direction, duration are not specified)
- Port scans monitoring (alert if port scans cross preset thresholds)

Enter the filter expression in the **Filter** text box on the **Alarm Configuration** screen,

Figure 3-4.

Figure 3-4: The Alarm Configuration screen



Traffic Analysis

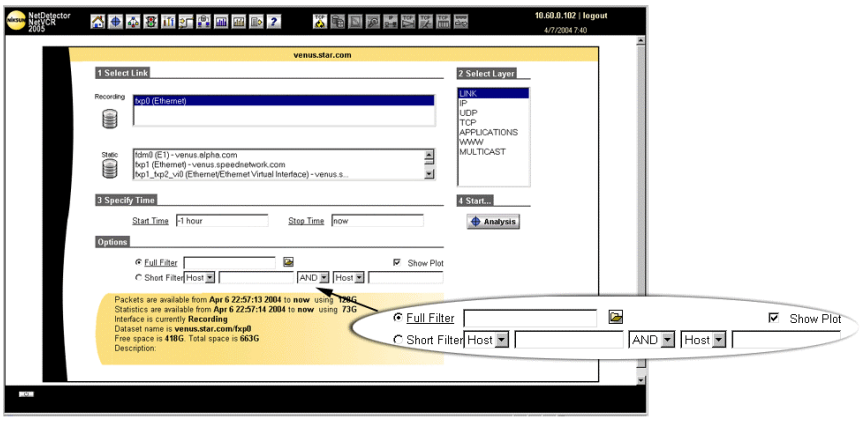
Filters are used in a number of Traffic Analysis features, as described below.

Analysis Start Screen

Applicable filter-type(s):

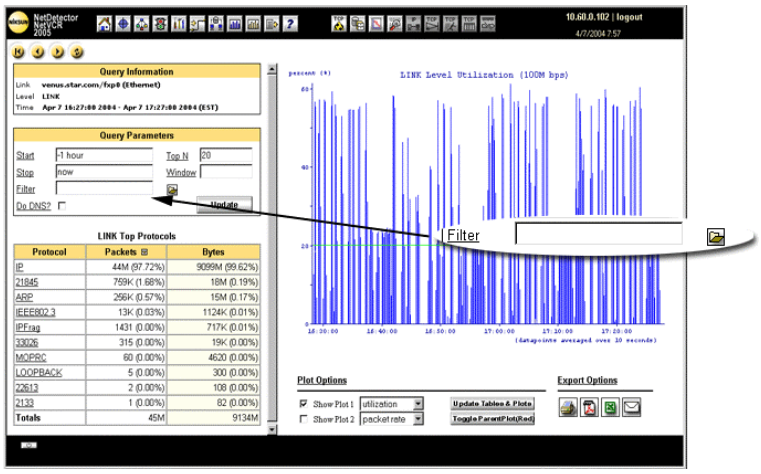
The **Start** screen (Figure 3-5) displays NetDetector/NetVCR's status and enables the user to enter basic filter expressions for analysis.

Figure 3-5: The Start screen



Enter filter expression in **Optional Filter** fields and click the **Analysis** button to view results on the **Traffic Analysis** screen (Figure 3-6).

Figure 3-6: The Analysis screen



Traffic Analysis: Main Screen

Applicable filter-type(s):

The **Traffic Analysis** screen (Figure 3-6), displays statistics, plots, and graphs at various levels of details, as specified by the filter expressions (entered on the **Start** screen).

On the **Traffic Analysis** screen, enter the filter expression in the **Filter** text box, and click the **Update** button to view the results. The **Traffic Analysis** screen enables you to drill-down through to multiple levels of detail. Filter expressions can be used in any of the levels, as described above. In the information box, on the top-left corner of the **Traffic Analysis** screen, the current filter expression is displayed.

Note: If the parameters in the filter expression are not compatible with currently selected data layers, no data is displayed.

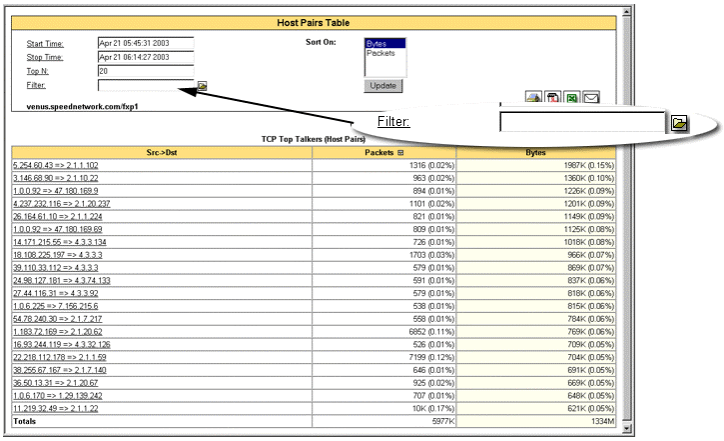
Host Pairs

Applicable filter-type(s):

On the IP Host Pairs screen

Figure 3-7, statistics filters can be used to qualify IP host pairs for the selected dataset and time-interval.

Figure 3-7: Host Pairs Tables screen

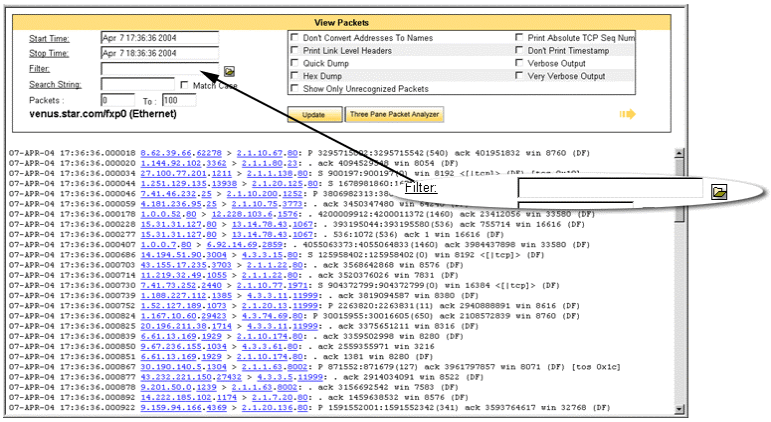


View Packets

Applicable filter-type(s):

Filtered data, at the packet level, can be viewed and exported in the PCAP format. The data to be exported can be filtered at the statistics and packet levels.

Figure 3-8: The View Packets screen

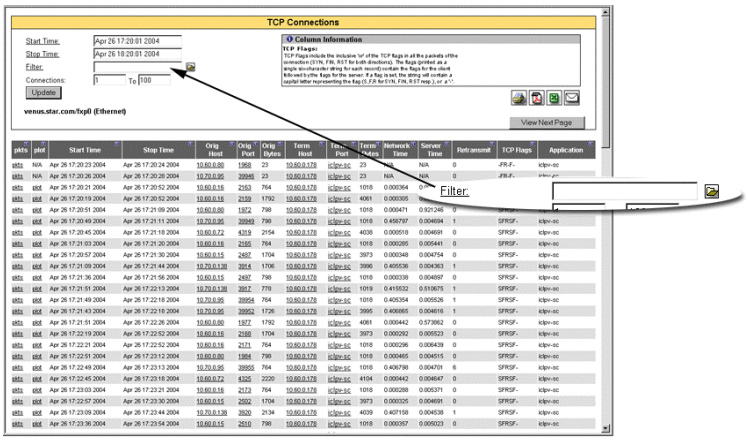


TCP Connections Tables

Applicable filter-type(s): S

On the TCP Connections screen statistics filters can be used to qualify hosts for the selected dataset and time-interval.

Figure 3-9: The TCP Connections screen S

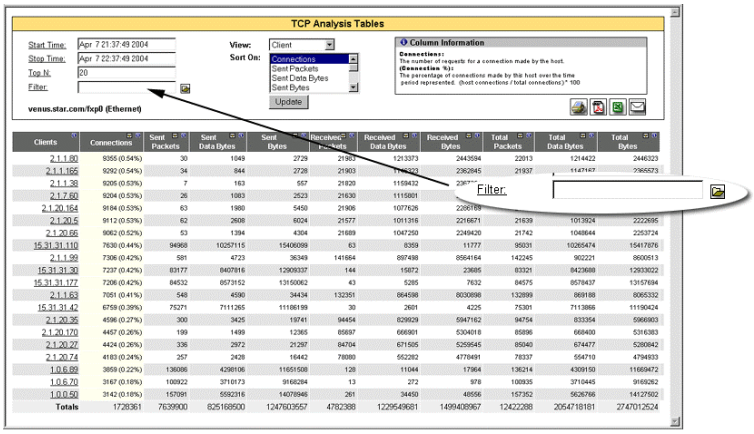


TCP Analysis Tables

Applicable filter-type(s): S

On the TCP Analysis Tables screen, statistics filters can be used to qualify hosts for the selected dataset and time-interval.

Figure 3-10: TCP Analysis tables S

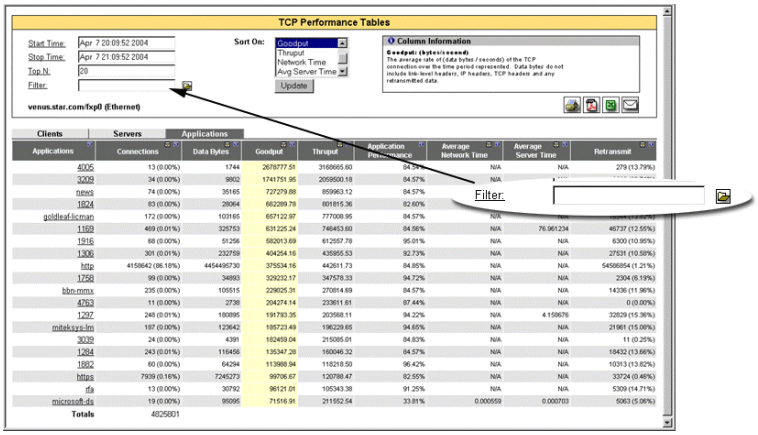


TCP Performance Tables

Applicable filter-type(s):

On the TCP Performance Tables screen (Figure 3-11), statistics filters can be used to qualify hosts for the selected dataset and time-interval.

Figure 3-11: TCP Performance Tables screen

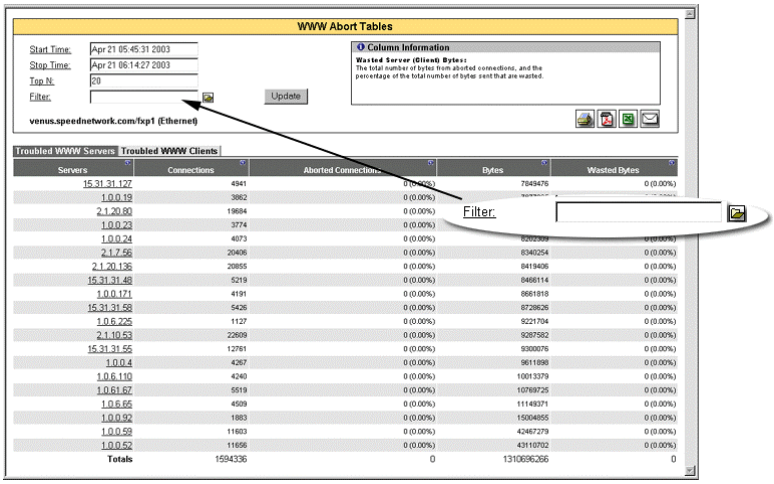


WWW Abort Tables

Applicable filter-type(s):

On the WWW Abort Tables screen (Figure 3-12), statistics filters can be used to qualify hosts for the selected dataset and time-interval.

Figure 3-12: WWW Abort Tables screen

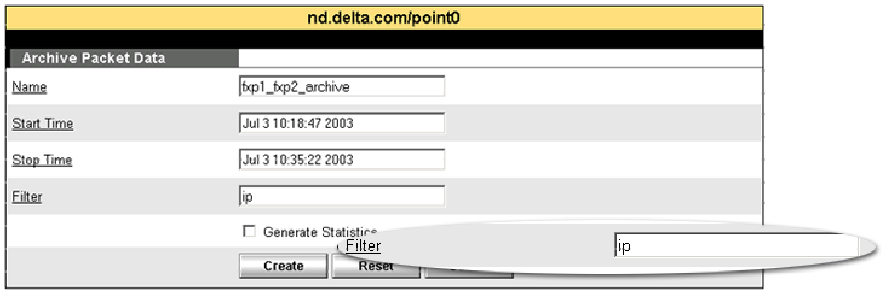


Archive Packet Data

Applicable filter-type(s): S P

Datasets can be filtered and archived (stored permanently). Filters can be applied on the screen as shown in Figure 3-13.

Figure 3-13: The Archive Packet Data screen S P

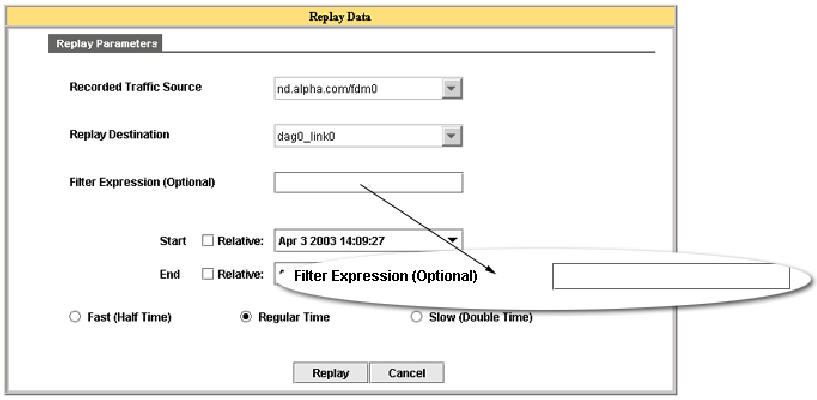


Replay Data

Applicable filter-type(s): S P

The **Replay Data** feature (Figure 3-14) enables users to replay any part of the dataset that has been filtered by the filter expression.

Figure 3-14: The Replay Data screen S P



Application Reconstruction

Applicable filter-type(s): S

Application Reconstruction (Figure 3-15) enables users to reconstruct selected portions of the recorded network traffic up to the TCP application level. Unusual traffic, including web pages and emails, can be reconstructed and displayed.

The application of filters enables users to selectively reconstruct traffic that is of interest. Figure 3-16 illustrates a reconstructed web page.

Figure 3-15: Application Reconstruction screen

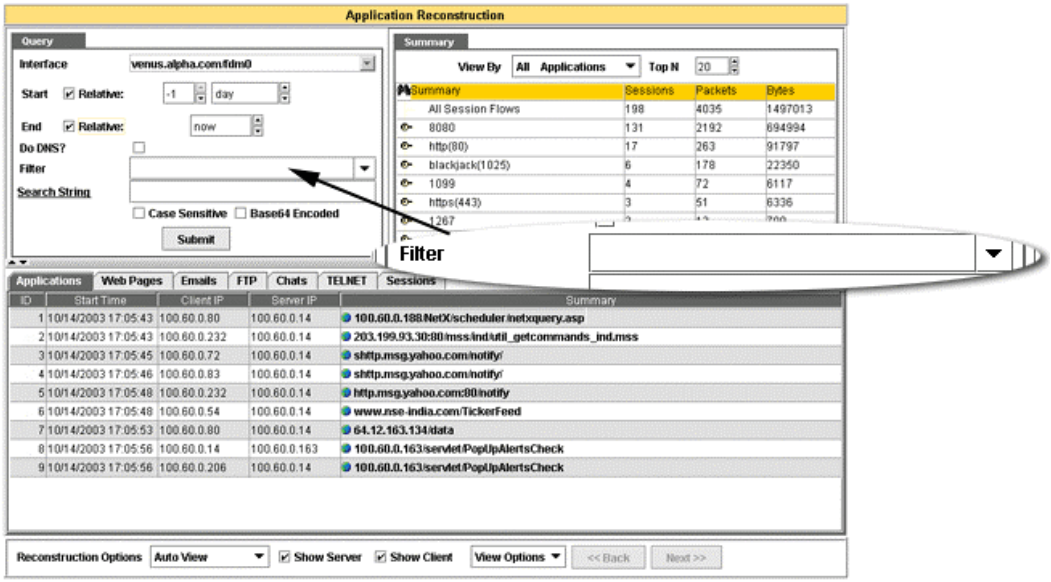
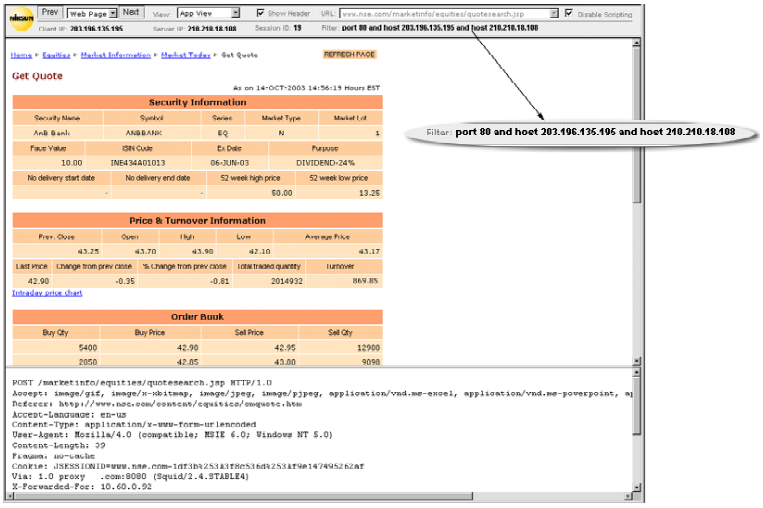


Figure 3-16: Reconstructed web page



Data Management

Filters can be applied by data management features to view, import, and export data. The features are described below.

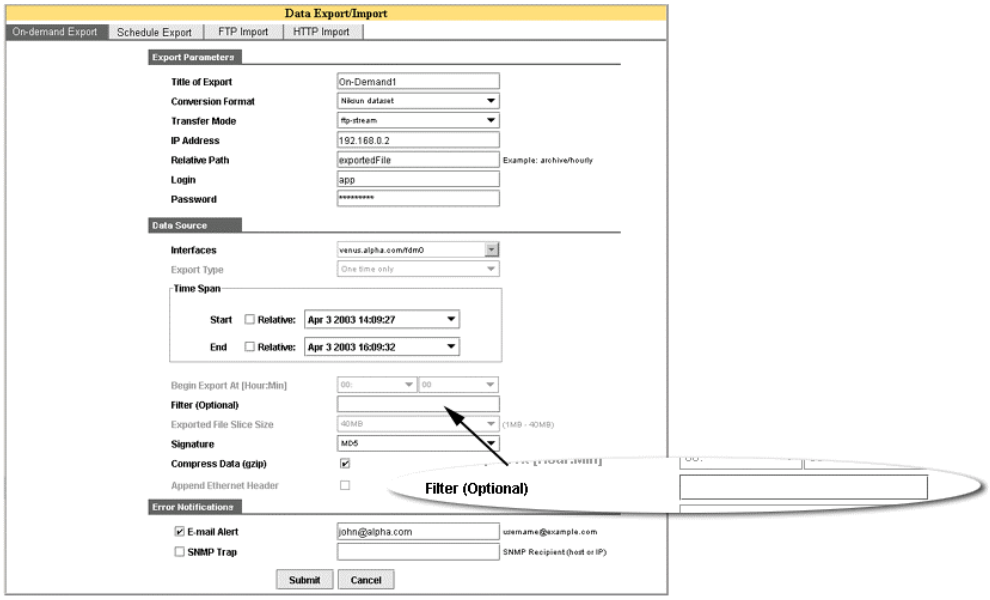
On-demand Export

Applicable filter-type(s):

NetDetector data management features enables users to transfer (import or export) specific intervals of recorded data to remote systems via HTTP and FTP.

The data to be exported can be filtered at the statistics and packet levels.

Figure 3-17: On-demand Export screen S P



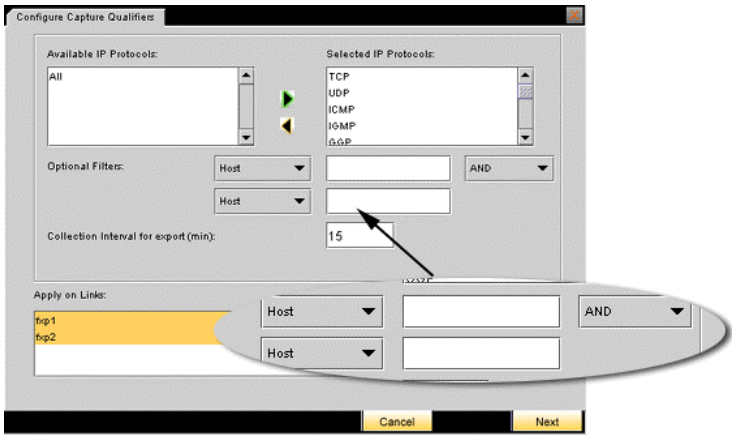
NetUsage

Applicable filter-type(s): S

The **NetUsage** utility enables users to export a subset of network traffic from the stored dataset.

Enter the filter expression in the **Optional Filters** boxes on the **Configure Capture Qualifiers** screen (Figure 3-18) to select portion of data that is of interest for export.

Figure 3-18: The NetUsage Configure Capture Qualifiers screen S



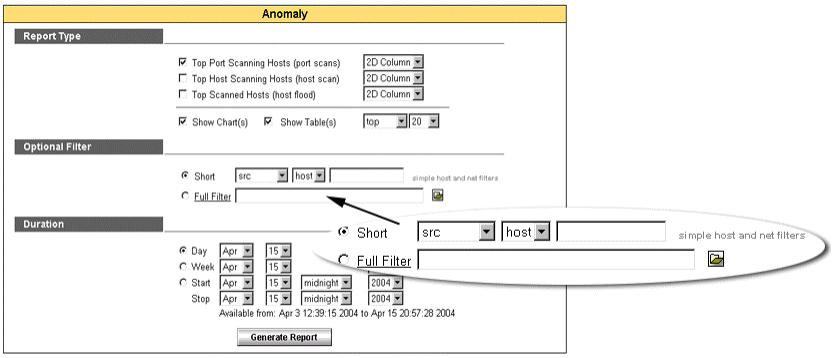
NetReporter for NetDetector

Applicable filter-type(s): S

NetReporter enables users to generate scheduled and on-demand reports on stored datasets. The reports can then be emailed to designated persons.

Enter the filter expression in the **Optional Filter** boxes, and click the **Generate Report** button on the **NetReporter** screen, to generate reports for the specified data.

Figure 3-19: The NetReporter screen S

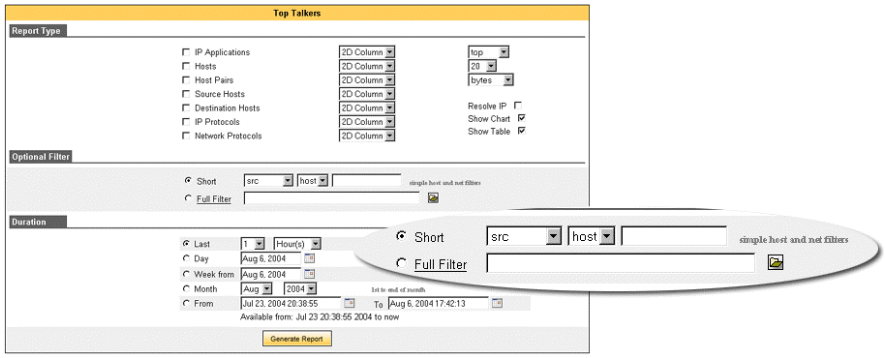


NetReporter for NetVCR

Applicable filter-type(s): S

Enter the filter expression in the **Optional Filter** boxes, and click the **Generate Report** button on the **NetReporter** screen, to generate reports for the specified data.

Figure 3-20: The NetReporter screen S



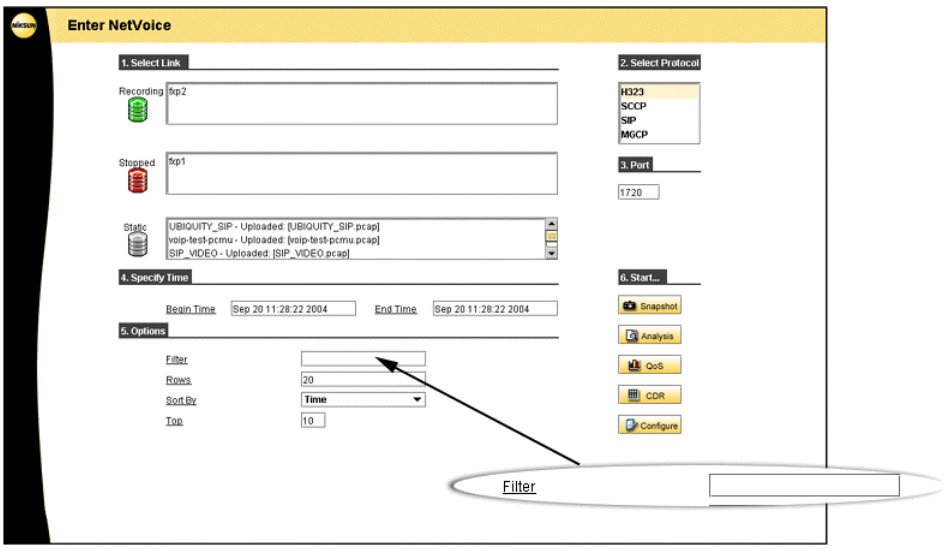
Using Filters in NetVoice

In NIKSUN NetVoice 2005, filter expressions are used in the following features:

- Viewing Snapshot
- Performing protocol analysis
- Providing Quality of Service (QoS) measurements
- Generating CDRs (Call Detail Records)

On the NetVoice Main screen, you can enter a user-defined filter expression.

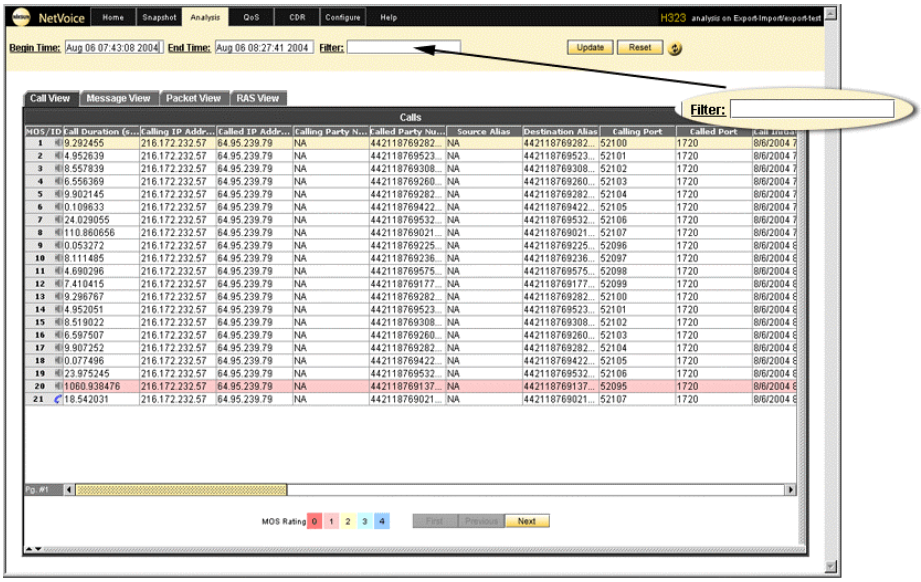
Figure 3-21: The NetVoice Main Screen



Clicking any of the buttons on the right side of the screen (except Configure), opens the corresponding screen with filtered data. For example, enter a filter in the main screen, and click the **Analysis** button. By default, the Call View screen opens displaying filtered call data.

The Call View screen is as shown.

Figure 3-22: Call View Screen



The Filter text box on this screen allows you to re-query on the basis of a new filter expression (or no filter) and refreshes the displayed data. You can apply filters for all the other options – Message View, Packet View, and RAS View.

Examples:

`proto \\tcp` analyzes all tcp packets

`proto \\udp` analyzes all udp packets

`host 10.0.0.40` analyzes all packets with host 10.0.0.40

`port 1720 or port 40499` will analyze packets from port 1720 or 40499

`calling_num==9810104202` filters all calls with this calling party number

`calling_num==981` filters all calls starting with this calling party number

`called_num == 9810104203` filters all calls with this called party number

`called_num==981` filters all calls starting with this called party number

`call_ref==12345` filters all calls with this call ID number

`call_ref==12` filters all calls starting with this call ID number

`rcode == "Normal call clearing"` filters all calls with this release cause code

`rcode == "Normal"` filters all calls starting with this release cause code

`duration >= 105` filters all calls with call duration > 105 secs

`mos < 4.0` filters all calls with call mos less than 4.0

Filters can be combined with the "or" or "and" operator.

Frequently Asked Questions

Question: Can "bit level" filtering, like the detailed filters applied on the View Packets screen, be applied to the recording filter?

Answer: Yes. All statistics and packet-level filters can be applied as a recording filter.

Question: How will that affect the performance of the box?

Answer: In general, complex and lengthy filter expressions that require many fields to be examined in each packet may impact performance while, on the other hand, simple filters that require very few fields to be examined in each packet may not impact performace.

Question: Can the same filters be applied to a virtual interface?

Answer: From the GUI, a virtual interface can be defined to represent a subset of traffic from the physical interface. It is important to note that recording filters are used while defining the virtual interface (In the document, all filters marked with the "R" icon can be used).

After the virtual interface has been created, separate statistics are generated for each virtual interface. The various features and screens see the virtual interface as any other interface. The same filtering rules then apply. For example, packet-level filters cannot be applied on the Analysis screen. In the Filters document, each of the icons describe where each of the filter types (i.e., recording, packet, statistics) can be applied.

Note: A "recording filter" is used only while defining the virtual interface and not at any other time. After the virtual interface has been created, for analysis and data management operations, valid statistics and packet filters can be used.

Note: Some RAID Installations will not have to run the disk check procedures described above.

About NIKSUN

NIKSUN is a recognized worldwide leader in developing and deploying a complete range of network performance monitoring, security surveillance and forensic analysis tools serving a wide range of protocols and interfaces, ranging from Ethernet and Gigabit Ethernet to OC-12. Our products are the only network appliances that continuously capture and analyze LAN, MAN and WAN traffic at Gigabit rates in a single platform.

NIKSUN's product line delivers unprecedented flexibility, scalability and real-time response. The company's patent-pending real-time data analysis and recording technology enables Enterprises, Governments, ASPs, ISPs and Carriers to provide secure and reliable network infrastructures and services.

NIKSUN is headquartered in New Jersey, USA and has sales offices in major cities throughout the U.S., Europe and Asia Pacific. In addition, NIKSUN has developed partnerships with industry leading network solution providers worldwide.

NIKSUN, Inc.
1100 Cornwall Road
Monmouth Junction
NJ 08852

Phone: +1-732-821-5000
Fax: +1-732-821-6000
Email: info@niksun.com

NIKSUN®

www.niksun.com